AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Samsung model S7 cellular telephone in a red Otter Box brand case, described in Attachment A, in evidence storage at the Federal Protective Service.

Case No. 3:20-mc-755

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Oregon
(identify the person or describe the property to be searched and give its location):

Samsung model S7 cellular telephone in a red Otter Box brand case, more fully described in Attachment A, in evidence storage at the Federal Protective Service Field Office in Portland, Oregon.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before August 12, 2020 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to U.S. Magistrate Judge Jolie Russo, via the Clerk's Office .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: July 29, 2020 11:15am

Jolie A. Russo
Judge's signature

City and state: Portland, Oregon

Honorable Jolie Russo, United States Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
3:20-mc-755	8/3/2020 1:10PM	

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Forensic extraction of Samsong S7 IMEI# 357752070860619.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 8/14/2020 1437 hrs

Executing officer's signature

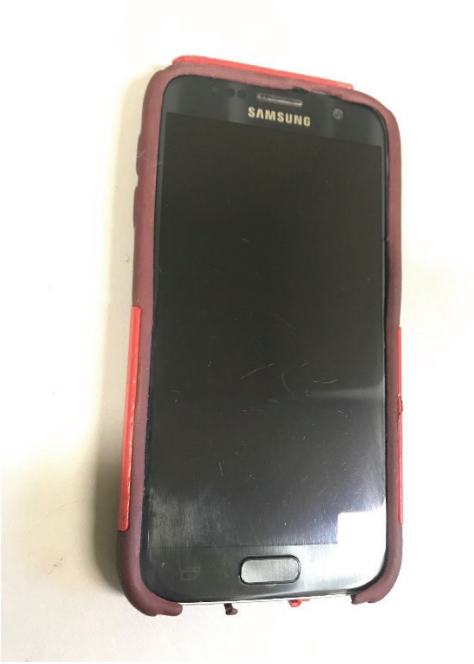
Micah Coving SA

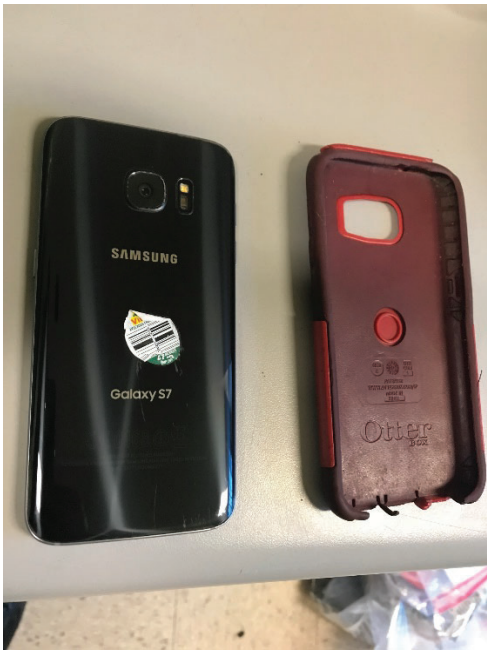
Printed name and title

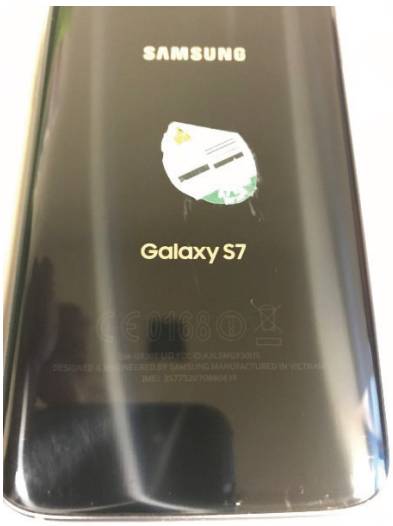
ATTACHMENT A

Item to be Searched

A black Samsung model S7 cellular telephone in a red Otter Box brand case, International Mobile Equipment Identity (IMEI) number 357752070860619, located at the Federal Protective Service (FPS) Field Office evidence storage in Portland, Oregon. Three photos of the phone follow:







ATTACHMENT B

Items to Be Seized

1. All data, files, images, and videos on the device described in Attachment A that relate to and are evidence of violations of 18 U.S.C. § 844(f)(1), involving the attempted arson of the Mark O. Hatfield U.S. Courthouse by Kevin Benjamin WEIER and at least one other unidentified individual, from June 13, 2020, to the present, including:

a. Text messages, available in both short message service and messaging applications, pertaining to the attempted arson of or other damage to the Hatfield Courthouse, or protest activities at the courthouse.

b. Photos and videos of WEIER or others damaging or attempting to damage the Hatfield Courthouse.

c. Photos and videos showing WEIER at or near the Hatfield Courthouse on or about July 12-13, 2020.

d. Logs of incoming or outgoing telephone calls, and the telephone numbers that called or were being called from the device, on or about July 12-13, 2020.

e. Calendar or travel information for WEIER for the month of July 2020.

2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

d. Information posted to social media accounts documenting WEIER's plans or preparations for committing the crime of arson, or his activities at the Hatfield Courthouse on or about July 12-13, 2020.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the device may require authorities to employ techniques, including computer-assisted scans of the entire medium, which might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the device will be performed within a reasonable amount of time not to exceed 120 days from the date of the warrant is executed. If the government needs additional time to conduct this review, it may seek an extension of that time period from the Court within the original 120-day period from the date the warrant is executed. The government shall complete this review within 180 days of the date the warrant is executed. If the government needs additional time to complete that review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the device does not contain any data falling within the ambit of the warrant, the government will return the device to its owner within a reasonable period of time following the search and will seal any image of the device, absent further authorization from the Court.

9. The government may retain the device if it contains contraband or evidence, if it is a fruit or an instrumentality of a crime, or to commence forfeiture proceedings against the device and/orthe data contained therein.

10. The government will retain a forensic image of the device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.